

REMARKS

Applicant has made clarifying amendments to claims 7, 11, 13-16. Applicant has also added new claims 18-31, which recite additional features of the invention. All of the claims are supported by Applicant's specification as filed.¹ No new matter has been added.

35 U.S.C §101

The examiner maintained the rejection of Claim 1 under 35 U.S.C. 101 because it is directed to a data structure. The examiner argued:

("A memory for storing a data structure for tracking network behavior, comprising: a connection table ...". When nonfunctional descriptive material is recorded on some memory, it is not statutory since no requisite functionality is present to satisfy the practical application requirement. Merely claiming nonfunctional descriptive material, i.e., abstract ideas, stored in a memory, does not make it statutory.)

In response to Applicant's arguments regarding the 101 rejection, the examiner merely repeats the claim, does not give any cogent reasons why the claim is non-statutory merely stating: "fits a data structure with mere arrangements of data in a table," and concludes that the claim is non-statutory. The examiner does not explain why he fails to follow the precedent that is binding on the examiner by offering any reasons why *Lowry* is distinguished from the instant case.

Applicant disagrees with the examiner's reason that: **Merely claiming nonfunctional descriptive material, i.e., abstract ideas, stored in a memory, does not make it statutory.**" First, the features of claim 1 are not non-functional; neither are they descriptive material nor abstract ideas. Rather, the data structure stored in the memory is tangible because it is embodied in the memory (hence it cannot be abstract) and is not non-functional, because it is used for tracking network behavior (as recited in the preamble), a real world application.

To further assist the examiner, the examiner's attention is directed to *In re Warmerdam*, 33 F.3d, 1354 31 USPQ2d 1754 (Fed. Cir.1994). In *Warmerdam*, the Federal Circuit found

¹ See for instance, Applicant's specification page 9, line 4 to page 12, line 28.

claims 1-4 and 6 reciting “steps [that] describe nothing more than the manipulation of basic mathematical constructs, the paradigmatic “abstract idea,”² non statutory. However, claim 5 directed to a computer having a specific data structure stored in memory was held to be statutory. The court observed that claim 5 was “a machine, and is clearly patentable subject matter.” 33 F.3d at 1360-61, 31 USPQ2d at 1759.

Unlike the situation in claims 1-4 and 6 in *Warmerdam*, instant claim 1 calls for a memory storing a data structure, the data structure for use with tracking network behavior. Thus, claim 1 calling for a memory recites statutory subject matter under 35 U.S.C. 101 and in agreement with both *Lowry* and *Warmerdam*. As in *Lowry*, these claims are: “More than mere abstraction, the data structures are specific electrical or magnetic structural elements in a memory.” *Lowry*, 32 F.3d at 1583-1584.

Double Patenting

The examiner provisionally rejected Claims 1-17 on the ground of non-statutory, obviousness-type double patenting as being unpatentable over claims 1-22 of co-pending Application No. 10701154 and claims 1-36 of co-pending Application No. 10701356.

The examiner stated:

Although the conflicting claims are not identical, they are not patentably distinct from each other a comparison between instant application independent claim 1 and the claims 1 and 14 (of the copending application number 10701154) and claims 1, 19, and 25 (of the copending application number 10701356) reveal the copending claims are simply species of the broader claim 1 of the instant application. Hence, claim 1 of the instant application is generic to the species of the invention covered by independent claims of the copending applications stated above. Thus, the broad generic invention is anticipated by the narrower species of the co-pending invention, thus without a terminal disclaimer, the species claims preclude issuance of the generic application. See *In re Goodman*, 11 F.3d 1046, 29 USPQ2d 2010 (Fed. Cir. 1993).

In response to Applicant’s argument, the examiner also stated that:

² “Nonfunctional descriptive material” includes but is not limited to music, literary works and a compilation or mere arrangement of data. Both types of “descriptive material” are nonstatutory when claimed as descriptive material per se. *Warmerdam*, 33 F.3d at 1360, 31 USPQ2d at 1759. When functional descriptive material is recorded on some computer-readable medium it becomes structurally and functionally interrelated to the medium and will be statutory in most cases since use of technology permits the function of the descriptive material to be realized.

Claims 1 and 14 of Copending Application 10/701154 and Claims 1, 19 and 25 of Copending Application 10/701356 contain every element of claim 1 of the instant application and as such anticipate(s) claim 1 of the instant application. Therefore, the narrower claims of the co-pending invention anticipate the broader claims of the instant application. See *In re Goodman*, 11 F.3d 1046, 29 USPQ2d 2010 (Fed. "A later patent claim is not patentably distinct from an earlier patent claim if the later claim is obvious over, or anticipated by, the earlier claim. *In re Longi*. 759 F.2d at 896, 225 USPQ at 651 (affirming a holding of obviousness-type double patenting because the claims at issue were obvious over claims in four prior art patents); *In re Berg*, 140 F.3d at 1437, 46 USPQ2d at 1233 (Fed. Cir. 1998) (affirming a holding of obviousness type double patenting where a patent application claim to a genus is anticipated by a patent claim to a species within that genus)." *ELI LILLY AND COMPANY v BARR LABORATORIES, INC.*, United States Court of Appeals for the Federal Circuit, ON PETITION FOR REHEARING EN BANC (DECIDED: May 30, 2001).

Present Application 10/701,155

Claim 1 of the present application is reproduced below: 1.

A memory device storing a data structure for tracking network behavior, comprising:

a connection table that maps each node of a network to a record that stores information about traffic to or from the node and between that node and others nodes in the network.

Co-pending Application 10/701,154

Claim 1 of the '154 matter is reproduced below:

1. A system, comprising:

a plurality of collector devices that are disposed to collect connection information to identify host connection pairs from packets that are sent between nodes on a network; and

an aggregator device that receives the connection information from the plurality of collector devices, and which produces a connection table that maps each node on the network to a record that stores information about packet traffic to or from the node, with the aggregator device further comprising:

a process executed on the aggregator device to detect anomalies in connection patterns; and

a process executed on the aggregator device to aggregate detected anomalies into the network events with the anomalies that are detected including denial of service attack anomalies and scanning attack anomalies.

Co-pending Application 10/701,356

Claim 1 of the '356 matter is reproduced below:

1. A device, comprising:
 - a processor;
 - a memory storing:
 - a connection table that maps each node of a network to a host object, the connection table stores information about traffic to or from the node; and
 - a process to detect anomalies based on information in the connection table and to aggregate the anomalies into the network events according to connection patterns.

Claim 1 of the present application is directed to memory device that stores a data structure for tracking network behavior. In contrast claim 1 of co-pending application '154, is directed to a system that includes a plurality of collector devices ... an aggregator device that receives the connection information from the plurality of collector devices ... a process ... to detect anomalies in connection patterns and a process ... to aggregate detected anomalies into the network events

Also, in contrast claim 1 of co-pending application '356 is directed to a device including a processor, a memory storing a connection table that maps each node of a network to a host object, the connection table stores information about traffic to or from the node and a process to detect anomalies based on information in the connection table and to aggregate the anomalies into the network events according to connection patterns.

Claim 1 of the instant application is directed to a data structure that stores a connection table. In contrast, claim 1 of the co-pending application '154 is directed to a technique that aggregates detected anomalies into network events that can correspond to denial of service attack and scanning attack anomalies. Also, in contrast, claim 1 of the co-pending application '356 is directed to detecting anomalies based on information in the connection table and aggregating the anomalies into the network events according to connection patterns.

The mere use of a connection table as elements in the claims of the co-pending application does not make the claims in the instant application either anticipated by or obvious

over the sets of claims of the co-pending applications because each of the sets of claims recite patentable distinct features of the connection table features are therefore directed to patentably distinct subject matter.

Therefore, the rejection is improper and should be removed.

35 U.S.C §102

The examiner maintained the rejection of Claims 1-9 and 11, 13-17 under 35 U.S.C. 102(e) as being anticipated by Tams et al U.S. Publication Number (20030069952), "Tams."

The examiner is referred to the office action for the text of his rejection because it is a repeat of the rejection made in the prior office action.

Claim 1

Claim 1 is allowable over Tams. In order for Tams to be a proper anticipating reference, Tams must disclose each and every element in claim 1, arranged as in claim 1. Tams fails to disclose a "data structure ... comprising ... a connection table that maps each node of a network to a record that stores information about traffic to or from the node and between that node and others nodes in the network."

The claimed "record feature" embodied in the memory of claim 1 is not suggested by any of the passages referred to by the examiner or elsewhere in Tams. Tams, for instance, whether in table 2 or the other tables, does not provide any mechanism to map each node of a network to a record that stores information ... to or from the node and between that node and other nodes in the network."

The examiner argues that: Tams teaches: "**a connection table (fig. 2, data table and Table 2, page 11) ...**" Applicant disagrees. The data table referred to in Tams does not store the claimed records (or an equivalent). Rather, as Tams mentions in [0161] "**the alMatrixTopN (Terminal Count Mode) table monitors conversations at all the known application-layer protocols, and stores them, using delta counters, in a table which is ordered by the packet or byte counters (depending upon user-configuration).**" As expressed in [0162] "**the user (or client program) [has requested] can request that the table be ordered by the byte counters,**" which gives the table depicted in Table 2, relied on by the examiner.

However, none of these elements in Table 2 is the claimed: “record that stores information about traffic to or from the node and between that node and others nodes in the network.” Rather, Tams merely stores IP addresses, packet counts and byte counts, but not the claimed record.

The table 2 on page 11 of Tams while showing IP addresses, and counters, does not “map[s] each node of a network to a record.” Rather, the table 2 is a listing of the different application protocols and packet/byte counts for those protocols.

Applicant does not agree that Tams describes connections, but assuming *arguendo* that the entries in Tams are connections, Applicant asks: Where does Table 2 have the traffic from the IP address “98.76.54.32” to the IP address “123.45.67.89”? That is, Tams does not have a record that provides traffic from IP address 98.76.54.32” to the IP address “123.45.67.89 and from the IP address “123.45.67.89 to the IP address 98.76.54.32” as would be needed to otherwise anticipate claim 1.

The examiner also argues Tams teaches: “maps each node of a network to a record object that stores information about traffic to or from the node and between that node and others nodes in the network (¶0157-0164 and ¶0210. See TABLE 2, page 11.” Applicant disagrees. Tams, in these paragraphs, discusses different ordering options for the contents of “alMartixTopN” table. However, this table (a version of which is depicted in table 2) does not “map[s] each node of a network to a record that stores information about traffic to or from the node and between that node and others nodes in the network.” In table 2, these entries are merely entries of source, destination addresses and counters. However, these entries are not mapped to a record that stores information about traffic to or from the node and between that node and others nodes in the network.

Accordingly, claim 1 is allowable over Tams. The remaining claims rejected as anticipated by Tams are allowable over Tams at least because they directly or indirectly from claim 1 and/or for the reasons discussed of record.

In response to Applicant’s argument, the examiner stated:

... Tams' Table 2 and ¶ 0210 show a connection table that maps each node (identified by an IP address 123.45.67.89) to a record object (host object/or destination IP address 98.76.54.32) and traffic information such as protocols used

(IP/TCP/FTP) and number of packets in the conversation between the hosts. Furthermore Tams teaches "Two conversations were detected during this first hourly time period. A first conversation between devices A and B which involved 10 packets and a second conversation between devices A and E which involved 6 packets. The number of bytes, in addition to the number of packets, may also be stored in each record of the database 707." (Para. 210).

The examiner takes the position that a record object (now a record) is "host object/or destination IP address 98.76.54.32." Nothing in Tams however suggests that nor has the examiner provided any cogent reasons why the IP address is the claimed record. The IP address is merely the IP address of the destination. Accessing the IP address does not return "... information about traffic to or from the node and between that node and others nodes in the network."

Clearly, Tams does not describe the claimed connection table because Tams builds a table that is ordered by either packet or byte counters. Tams' data is organized by byte/packet count. That is, the RMON2 tables of interest (e.g., alMatrixTopN, etc.) track the "top" pair-wise protocols, rather than organize records by host or host-pairs. The claimed connection table lets a user access all traffic to/from a host (or between hostpairs), optionally broken down by protocol, as in the dependant claims, rather than looking at a list of protocol/hostpair rows sorted by traffic volume, as in the case with Tams.

However, even were Tams to be reorganized, Tams' data does not reflect all traffic to/from a host. See for example [0086]-[0087] of Tams.

In short, the connection table is a mechanism to represent traffic on a network connection based manner, whereas Tams is focused on aggregating data specifically from RMON2 probes, and transforming different kinds of RMON formats into one format (the alMatrixTopN format).

Claims 2 and 3

The examiner argues: "As per claims 2 and 3, Tams teaches wherein the connection table includes a plurality of records that are indexed by source and destination address (See TABLE2, page 11)." Applicant disagrees. Table 2 shows the table indexed by "Network Layer Protocol." Tams describes this also in paragraph 0161.

The examiner in response to Applicant's argument states:

The Examiner respectfully disagrees. The Applicant did not explain how a table listing traffic information between nodes by source and destination address as shown by Tarn's table 2 is different the Applicant's claimed connection table. Examiner believes Tarn's table 2 meets the Applicant's argued limitation. As to indexing by time, Tarn clearly show time stamp traffic information indicating the conversation between hosts that is stored in a database by different time interval. See Tf0198 and 10201-0208 and the time scale data structure 709,711,713 and 715 in fig. 7.

Applicant disagrees. Applicant has clearly argued the feature of the "record." Tarn does not have such a feature making at best the discussion of source address and destination address data that are stored in Tarn's disclosed table.

Claim 4

The examiner argues: "As per claim 4, Tarn teaches the device of claim 1 wherein the connection table includes a plurality of records that are indexed by time ([0198] and [0201-0206]; see steps in fig. 8)." Applicant disagrees that Tarn describes the claimed connection table.

Claim 5

The examiner argues: "As per claim 5, Tarn teaches the device of claim 1 wherein the connection table includes a plurality of records that are indexed by source address, destination address and time (See TABLE 2, page 11 and [0198] and [0201-0206])." Applicant disagrees. Table 2 does not show records indexed by source address or destination address. According to Tarn [0161] "the aIMatrixTopN (Terminal Count Mode) table monitors conversations at all the known application-layer protocols, and stores them, using delta counters, in a table which is ordered by the packet or byte counters (depending upon user-configuration)." As expressed in [0162] "the user (or client program) [has requested] can request that the table be ordered by the byte counters," which gives the table depicted in Table 2 relied on by the examiner. Tarn says nothing about indexing by source address or destination address in discussion of Table 2 or in the discussion of the time granularity in [0198] and [0201 to 0206].

Claims 6 and 7

The examiner argues: "As per claim 6, Tarn teaches the device of claim 1 wherein the connection table is a plurality of connection sub-tables each sub-table having data pertaining to network traffic over different time scales (10198 and 10201-0208; see the time scale data structure (709, 711, 713 and 715 in fig. 7)." Claim 6 is allowable

over Tams at least because the structures relied on by Tams, namely, “(709, 711, 713 and 715 in fig. 7)” do not suggest the features of the connection table.

Claim 8 is allowable for analogous reasons as given for claim 6.

Claim 9 is allowable for analogous reasons as given for claim 5.

Claim 11

The examiner argues: “As per claim 11, Tams teaches the device of claim 1 wherein the host record of a first host also maps to a second host which communicates with the first host to a “host pair record” that has information about all the traffic from between the first and second hosts ([0201] and [0209-0210]). Applicant disagrees. Claim 11 specifies details of the “host pair record.” It requires that it possess all information from the first to the second host and from the second to the first host. The examiner relies on passages from Tams that describe and depict individual records of different “conversations,” but neither describe nor suggest the claimed host pair record.

Claim 13

The examiner argues: “As per claim 13, Tams teaches the device of claim 1 wherein a record stores a measure of the number of bytes, packets, and connections that occurred between hosts during a given time-period (1 0157-0164 and 10210. See TABLE2, page 11).” Applicant has amended claim 13 to clarify the claim. Claim 13 now calls for “... the connection table comprises a plurality of host records a host record stores a measure of the number of bytes, packets, and connections that occurred between hosts during a time-period.” Arguably, Tams discusses records of some sort, however Tams does not describe the records of claim 13 because Tams does not disclose records that stores a measure of “...connections that occurred between hosts”

Claim 14

The examiner argues: As per claim 14, Tams teaches wherein data in the record is organized by well known transport protocols and well-known application-level protocols (1 0151-0157 and 10161-168. See TABLE 2 and TABLE 4A-4B in page 11). Applicant disagrees. Claim 14 has been amended to depend from claim 13, and requires that data in the host record is organized by well known transport protocols and well-known application-level protocols. Tams does not describe that data in the host record is

organized by well known transport protocols and well-known application-level protocols, albeit Tams does mention transport protocols and application-level protocols.

Moreover, the table does not make it easy to do arbitrary protocol queries, because it contains rows only for the "top-most" protocols.

For example, if a host sends 10 raw IP packets, 10 TCP/IP packets, and 10 TCP/IP/HTTP packets, the table will only report 10 packets when queried for "IP", rather than accounting for packets that IP encapsulates (total of 30). In other words, there is no easy mechanism to retrieve all of the IP statistics.

Claims 15-17 are allowable at least for the reasons discussed in their respective base claims.

35 U.S.C §103

The examiner rejected Claim 10 under 35 U.S.C. 103(a) as being unpatentable over Tams in view of Maufer et al U.S. Patent Number (7120930), hereinafter "Maufer."

Claim 10 includes the feature that "the addresses indexing the connection include a physical layer address to IP address map that is used to determine Host ID."

Applicant contends that no combination of Tams with Maufer suggests the features of claim 10. Maufer does not teach "the addresses indexing the connection include a physical layer address to IP address map that is used to determine Host ID" as the examiner argues but instead discloses mapping between active clients and gateway managed public IP addresses. However, while discussing mapping, Maufer clearly does not teach any mapping for use in a connection table of the type claimed in claim 1 for the function to determine Host ID in the connection table.

Therefore Maufer does not teach the added feature of claim 10 and does not cure the deficiencies in the base reference, Tams.

The examiner rejected Claim 12 under 35 U.S.C. 103(a) as being unpatentable over Tams in view of Ontiveros et al U.S. Patent Number (20020107953), hereinafter "Ontiveros".

The examiner argues that:

As per claim 12, although Tams shows substantial features of the claimed invention including a connection table that enables a consuming device to obtain summary information about one host and about the traffic between any pair of hosts (10118), Tams does not explicitly show a two level mapping between a first one of the hosts of any pair to a second one of the hosts of the any pair and from the second one of the host of the any pair to the first one of the host for the any pair for a second level mapping.

Nonetheless, this feature is well known in the art and would have been an obvious modification of the system disclosed by Tams, as evidenced by Ontiveros U.S. Pub Number (20020107953).

In analogous art, Ontiveros discloses a two level mapping between a first one of the hosts of any pair to a second one of the hosts of the any pair and from the second one of the host of the any pair to the first one of the host for the any pair for a second level mapping (¶ 036-050 and abstract).

Giving the teaching of Ontiveros, a person of ordinary skill in the art would have readily recognized the advantage of modifying Tams by employing the data traffic monitoring system of Ontiveros in order to detect any suspicious packets in any direction (both incoming and outgoing) of the network data traffic. In this way unauthorized access to a network is recognized and prevented.

Claim 12, which requires the features of "... the connection table includes two level mapping that enables a consuming device to obtain summary information about one host for a first level mapping and about the traffic between any pair of hosts, in either direction, between a first one of the hosts of the any pair to a second one of the hosts of the any pair and from the second one of the hosts of the any pair to the first one of the hosts of the any pair for a second level mapping."

The examiner acknowledges that Tams does not describe this feature and relies on Ontiveros.

The examiner does not specify what in Ontiveros describes the claimed feature.³ The examiner improperly requires Applicant to speculate where the examiner contends the teaching is specifically found.

As an example Ontiveros [0040] is reproduced below:

[0040] With respect more specifically to the "hit-count" table, each time a data packet is received, a preferred algorithm as described herein creates a new reference index (if one does not already exist) or increments the existing reference (i.e., counting packets). For example, as shown at 100 in FIG. 2, the packet daemon identifies the packet source address qw1232ewr23 and at 102 creates a memory reference (memref) for that source address. At 104 the packet daemon identifies the source address of the next data packet traversing the port being monitored by the packet daemon, in FIG. 2, the source address being mg32ewr009. At 106 another

³ The examiner argues that the teaching is buried somewhere in (¶ 036-050 and abstract) of Ontiveros.

memref is created for this source address. Therefore, at 104 each of the memrefs are equal to 1, representing that one data packet from each of the sources identified has traversed the data port of interest. At 108, another packet from source address gw123ewr23 is identified, and as shown at 110, the corresponding memref for that address is incremented. So, if for example the threshold data packet value is 1000 for the sample time (e.g., 10 milliseconds), and source address gw123ewr23 exceeds the threshold in this period (e.g., memref gw123ewr23=1001), then access to the port being monitored will be denied to packets from that source. It should be noted that the source may be transmitting from either outside or inside the network.

Neither in [0040] nor elsewhere in Ontiveros in particular [0036-0050] does Ontiveros have any structure that corresponds to the connection table and in particular a connection table that includes “two level mapping that enables a consuming device to obtain summary information about one host for a first level mapping and about the traffic between any pair of hosts, in either direction, between a first one of the hosts of the any pair to a second one of the hosts of the any pair and from the second one of the hosts of the any pair to the first one of the hosts of the any pair for a second level mapping.”

Applicant presumes that the examiner uses the teachings of the hit-count table. The hit-count table is as its name implies, counts the number of times that a pair of source and destination addresses is detected. Ontiveros states:

A "hit-count" table is preferably created in memory to count the number of times a particular pair of source and destination IP addresses is detected. Entries are stored using a hash table, keyed by the source and destination addresses. In operation, if the "hit" count exceeds a configurable threshold, all traffic between the source and destination endpoints is disabled for a configurable lockout period. When the lockout period ends, traffic between the endpoints is re-enabled. The IDS of the monitoring system 50 preferably generates a system log message when a lockout period begins or ends.

Thus, while the hit-count table tracks the number of times a particular pair of source and destination IP addresses is detected, the hit count table neither possess the features of the connection table nor the claimed “two level mapping . . .”

The examiner is also directed to Ontiveros, Fig. 2, reproduced below, which shows that the hit-count table of Ontiveros is not the functional equivalent of the connection table.

Patent Application Publication Aug. 8, 2002 Sheet 2 of 9 US 2002/0167953.

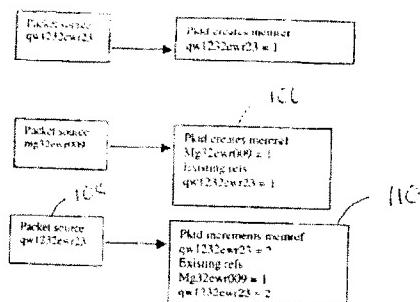


FIG. 2.

As Ontiveros [0040] explains, "Therefore, at 104 each of the memrefs are equal to 1, representing that one data packet from each of the sources identified has traversed the data port of interest. At 108, another packet from source address gw123ewr23 is identified, and as shown at 110, the corresponding memref for that address is incremented." Therefore, it is clear that nothing in Ontiveros [0040], Fig. 2 or elsewhere suggests the claimed connection table with the claimed "two level mapping."

If the examiner chooses to persist in this line of reasoning Applicant contends that it is incumbent upon the examiner to specifically point out the relevant features from Ontiveros.

Accordingly, claim 11 is further allowable over Tams combined with Ontiveros because no combination of the references suggests the claim feature.

It is believed that all the rejections and/or objections raised by the examiner have been addressed.

In view of the foregoing remarks, applicant respectfully submits that the application is in condition for allowance and such action is respectfully requested at the examiner's earliest convenience.

All of the dependent claims are patentable for at least the reasons for which the claims on which they depend are patentable.

Canceled claims, if any, have been canceled without prejudice or disclaimer.

Any circumstance in which the applicant has (a) addressed certain comments of the examiner does not mean that the applicant concedes other comments of the examiner, (b) made

Applicant : Massimiliano Antonio Poletto et al.
Serial No. : 10/701,155
Filed : November 3, 2003
Page : 20 of 20

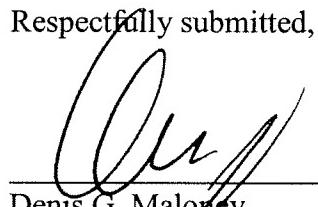
Attorney's Docket No.: 12221-025001

arguments for the patentability of some claims does not mean that there are not other good reasons for patentability of those claims and other claims, or (c) amended or canceled a claim does not mean that the applicant concedes any of the examiner's positions with respect to that claim or other claims.

No fee is due. Please apply any other charges or credits to deposit account 06-1050.

Respectfully submitted,

Date: 6/19/04


Denis G. Maloney
Reg. No. 29,670

Fish & Richardson P.C.
225 Franklin Street
Boston, MA 02110
Telephone: (617) 542-5070
Facsimile: (617) 542-8906